Medical Mobile Apps Data Security Overview

Ceara Treacy, Fergal McCaffery
Regulated Software Research Centre & Lero
Dundalk Institute of Technology,
Dundalk, Ireland
e-mail: {ceara.treacy, fergal.mccaffery }@dkit.ie

***Abstract*— In the growing industry of mHealth, mobile medical apps are becoming a popular mechanism for healthcare delivery. Characteristically, these apps are designed to both process and transmit data that is sensitive medical data. Such data is required to be kept private and secure through regulations and legislation. The detections of increased app hacking by security companies and researchers are especially significant amidst today's rapid growth in healthcare mobile apps. Consequently, security and integrity of the data associated with these apps is a growing concern for the app industry, particularly in the highly regulated medical domain. Until recently, data integrity and security in transmission has not been given serious consideration in the development of mobile medical apps. There are currently no procedures or standard practices for developers of mobile medical apps to assure data integrity and security in transmission. This paper is an overview of existing mobile medical apps data security issues and security practices. We discuss current regulations, standards and best practices concerning data security in mobile medical apps. The paper introduces the concept of a process model and testing suite to assist mobile medical app developers to implement data security requirements to assure the Confidentiality, Integrity and Availability of data in transmission.**

Keywords-Mobile Medical Apps; data security; regulations; data security testing.

I. INTRODUCTION

In mHealth, mobile apps are generally classified into mobile health/wellbeing apps (MHAs) and mobile medical apps (MMAs). A MMA is an app that qualifies as a medical device and is therefore required to follow the applicable medical device regulatory requirements. Medical professionals and the general public use mobile apps to perform many tasks, such as: health and fitness tracking, sharing medical videos, photos and x-rays; blogs to post medical cases and images; share personal health information; and keep track of alerts on specific medical conditions and interests [1]. MMAs are evolving quickly with the processing capabilities of mobile devices. The use of mobile apps enables dynamic access to personal identifiable information and the collection of greater amounts of sensitive data relating to personal health information (PHI). The use of mobile apps implicates changes in the way health data will be managed, as the data moves away from central systems located in the services of healthcare providers, to apps on mobile devices [2]. Increasing reliance on mobile apps raises questions about compromised patient privacy [3] and security of the data accompanying the apps [2]. The PwC's Health Research Institute's survey claims 78% of surveyed consumers were worried about medical data security, while 68% were concerned about the security of their data in mobile apps [4].

The impact of data breaches in the medical industry is far-reaching in terms of costs, losses in reputation [5] and potential risk to patient safety. Reasons for obtaining access to PHI can be for monetary aim, harmful and personal intention [6]. An example of the importance of cybersecurity can be seen with the health insurer Anthem in the US. A reported breach involved hackers obtaining personal identifiable information and PHI for about 80 million of its customers and employees [7]. The information stolen falls under the Health Insurance Portability and Accountability Act (HIPAA), which is the federal law governing the security of medical data and could result in fines up to $1.5million. A data breach that maliciously makes changes to a medical diagnosis or prescribed medication has serious consequences in terms of physical harm and patient safety. With PHI breaches, either through physician diagnosis or a treatment plan, the possibility of personal harm or loss is pronounced.

The Food and Drug Administration (FDA) regulates medical devices in the U.S and are alert to the cybersecurity of medical devices. In July 2015, the FDA issued a cybersecurity alert to users of a Hospira Symbiq Infusion System pump, where it strongly recommended discontinued use, as it could be hacked and dosage changed [8]. In September 2015, the FBI issued a cybersecurity alert, outlining how Internet of Things (IoT) devices may be a target for cybercrimes and may put users at risk [9]. If a cyber-thief changes patient medical information or a physician diagnosis, serious medical harm or even death can result. An article that references the DarkNet, describes how it is now possible to purchase a medical identity that mirrors individual ailments, size, age and gender, to seek "free" medical services that would not be suspicious to a clinician. It states this type of crime is estimated to cost the healthcare industry in the US between $35 billion and $80 billion each year [10].

It is largely assumed MMAs are not typically deployed in "hacker rich" mobile environments [11]. However, Arxan research shows that many sensitive medical and healthcare apps have been hacked with 22% of these being FDA approved apps [11]. MMA developers do not have extensive experience with the types of threats other consumer app industries (e.g., banking) are familiar with. Consequently, security and privacy has not been given serious consideration until recently, while the importance of security is getting recognized little is yet being done [12]. Development of MMAs is picking up momentum as many companies are lured into the domain by the explosion of the market and the

potential financial gains. However, issues arise such as: many of these developers are not coming from the highly regulated medical device domain and are not aware of the data protection and privacy requirements of PHI. Developers coming from the medical device domain are discovering the technical complications of entering the mobile domain. The European Commission's 'Green Paper on mHealth', findings are that this market is dominated by individuals or small companies, with 30% being individuals and 34.3% are small companies (defined as having 2-9 employees) [13]. This would advocate a lack of experience, knowledge and financial means to address the issues outlined above. The research aims to assist developers address privacy and security of data for MMAs, drawing from the standards and best practice perspectives.

This paper is organized as follows: Section II covers background on MMAs and data transmission. This section also discusses MMA security matters. Section III, outlines the privacy and security laws for health data. In Section IV, we introduce our research of a process model to assure the Confidentiality, Integrity and Availability (CIA) of data in transmission for developers of MMAs. Finally, we conclude the paper and present the future work in Section V.

II. BACKGOUND

A. MMAs and Data Transmission

In July 2011, the FDA issued draft guidance for MMAs and defined a "mobile medical app" as a software application run on a mobile platform (mobile phones, tablets, notebooks and other mobile devices) that is either used as an accessory to a regulated medical device or transforms a mobile platform into a regulated medical device and can be used in the diagnosis, treatment, or prevention of disease [14].

Mobile devices now provide many of the capabilities of traditional PCs with the additional benefit of a large selection of connectivity options [15]. Mobile devices typically connect to wireless sensor networks, which are being used in a wide range of medical and healthcare apps [16]. Wireless Body Area Networks (WBAN) emerged in order to address the growing field of sensor technologies. A WBAN is a purpose sensor network that operates independently to connect to various medical sensors and appliances, located inside and outside of a human body [17]. The information is transmitted via independent nodes that collect sensitive (life-critical) information [18]. A Task Group IEEE 802.15.61, was established for the standardization of WBAN. The current IEEE 802.15.6 standard purpose was to define new Physical (PHY) and Medium Access Control (MAC) layers for WBAN and defines three PHY layers; Narrowband (NB), Ultra wideband (UWB), and Human Body Communications (HBC) layers. The selection of each PHY depends on the application requirements.

Currently, technologies used for data transmission include Bluetooth/ Bluetooth Low Energy, ZigBee, UWB, Wireless Medical Telemetry Service (WMTS), communication networks such as WiFi (WLAN) and mobile data networks 3G & 4G. Data is transmitted to and from the MMA or to sensors on a personal health device or a medical device. Other transmission of data may occur between the MMA and for example: remote Health/Service Centers; Medical Professionals; or Health Record Networks. In some cases, the information sent to the MMA is processed on the app and retransmitted to the specified device or center. Through MMAs the collection of significant medical, physiological, lifestyle and daily activity data [13] is greatly amplified and transmitted via varied and numerous networks.

B. Mobile Medical Application Security

Security and privacy related to patient data are two essential components for MMAs. The fundamental concepts when considering data security are confidentiality, integrity and availability. Confidentiality is protection of the information from disclosure to unauthorized parties. Integrity refers to protecting information from being modified by unauthorized parties. Availability is ensuring that authorized parties are able to access the information when needed. When considering data security risks for MMAs it is necessary to specify what types of security threats they should be protected against. Deployment of MMAs involves security threats from multiple threat sources which include: attacks; the user; other mobile apps; network carriers; operating systems and mobile platforms. These security risks are further extended when consideration is given to the unauthorized access to the functionality of supporting devices and unauthorized access to the data stored on supporting devices [19]. The 2015 Ponemon report on mobile app security, emphasized that not enough is spent on mobile app security [20].

1) Attacks: Attacks are the techniques that attackers use to exploit the vulnerabilities in applications. There are numerous tools available for hacking into MMAs and wireless networks. Hackers target mobile apps to gain entry into servers or databases in the form of malware attacks. A recent list of these tools can be found in the Appendix of the Araxan Report [11]. This report examined 20 sensitive medical and healthcare apps and discovered 90% of Android apps and no iOS apps have been subject to hacking [11]. When data travels across a network, they are susceptible to being read, altered, or "hijacked". Potential for breaches of confidentiality of data occurs during collection and transmission of data. Data in transmission to and from the MMAs must be protected from hacking. Some of the most common issues (but not inclusive) are Easvesdropping, Malware, Node Compromise, Packet Injection, Secure Localization, Secure Management, Sniffing Attacks, Denial of Service (DoS), SQL injection attacks, Code Injection and Man-in-the Middle attacks. The consideration of WBANs for MMAs must satisfy rigorous security and privacy requirements [18]. Wireless channels are open to everyone. Monitoring and participation in the communication in a wireless channel can be done with a radio interface configured at the same frequency band [21]. This may cause severe damage to the patient since the cybercriminal can use the attained data [18] for many of the illegal purposes mentioned above. The ISO/IEEE 11073 standard deals only with mutual communication protocols and frameworks exchanged between and has never

considered security elements until recently, irrespective of all sorts of security breaches [22]. Security issues must be resolved while designing medical and healthcare apps for sensor networks to avoid data security issues [16].

2) Users: Many of the mobile devices will be personal and bypass the majority of inbound filters normally associated with corporate devices which leaves them vulnerable to malware. It is important that the user has good knowledge of the security safeguards, what measures to follow and what precautions to take [23]. A key challenge with MMA data is the lack of security software installed on mobile devices [24]. Many mobile device users do not avail of or are unacquainted with basic technical security measures, such as firewalls, antivirus and security software measures. Mobile device operating systems are very complex and therefore demand additional security controls for the prevention and detection of attacks against them [25]. The accessibility of social media and email make it easy to post or share information in violation of HIPAA regulations. An example being, a New York nurse was fired because she posted a photo to Instagram of a trauma room after treating a patient [26]. Mixed with the availability to mobile phone cameras and social media apps, the risk of employees divulging PHI and violating HIPAA requirements has increased [27]. One of the greatest threats to MMA data security lies with the fact that most are on mobile devices which are portable, making them much more likely to be lost or stolen [28]. Potentially any data on the device is accessible to the thief, including access to any data and hospital networks. Due to the regulatory protection of PHI, it is important that even when the app is on a stolen device the security of the data remains protected and is regularly backed-up [25]. Measures should be available to remotely lock the MMA, disable service, completely wipe out the data [25] and restrict access to supporting devices.

Not all users password-protect their devices. Even when passwords are used because of the lack of physical keyboards with mobile devices, users tends not use complex passwords to secure their information. The use of more than one type of authentication technique suggested by Alqahtani, would afford better data security for MMAs [25]. The difficulty is requesting lengthened authentication requirements from a busy medical professional. Inputting numerous passwords, or waiting for an authentication code in a pressurized situation is not desirable.

3) Other mobile apps: Unfortunately, many users download mobile apps often without considering the security implications. Unintentionally, a user can download malware in the form of another application, an update or by downloading from an unauthorised source. The difficulty in detecting the attack was due to the fact that there currently is no mobile device management application programming interface (API) to obtain the certificate information for each app [29]. An attacker can use Masque Attacks to bypass the normal app sandbox and get root privileges by attacking known iOS vulnerabilities [29]. Cloned apps are a concern, over 50% of cloned apps are malicious and therefore pose serious risks. A recently discovered iOS banking app malware, Masque Attacks, replace an authentic app with malware that has an identical UI. The Masque Attacks access the original app's local data, which wasn't removed when the original app was replaced and steal the sensitive data [29]. The mobile device management interface did not distinguish the malware from the original as it had used the same bundle identifier.

4) Operating systems & devlopment: Consideration with handling data on mobile devices includes unintended data leakage. It is essential that the MMA is not susceptible to analytic providers that will sell the data to marketing companies. The app stores are attempting to address this, e.g., Apple is banning app developers from selling HealthKit data or storing it on iCloud. Google insists that the user is in control of health data as apps cannot be accessed without the user providing permission. Developers could include analytics that report how often a section of the MMA was viewed, similar to the analytics credit card provider's use to flag unwanted access to data. It is equally important to consider the intentional or unintentional sharing of personal information. Leakage of personal data from the device to the MMA and the leakage of MMA data onto personal devices are key considerations. The bypass of outbound filters elevate the risk of non-compliance with data privacy laws and requirements, e.g., the use of personal Dropbox.

A basic requirement such as encryption is not used in many apps. Data is encrypted so that it is not disclosed whilst in transit. Data encryption service provides confidentiality against attacks. The requirement of encryption is stressed, not only for the data, but for the code in development to assure data security [16][25]. Data encryption of passwords and usernames if they are to be storage on the MMA is essential, many apps store this information in unencrypted text. This means that anyone with access to the mobile device the MMA resides on can see passwords and usernames by connecting the device to a PC. If the MMA is hacked, the information encrypted will be useless to the cybercriminals. Many apps send data over an HTTPS connection without checking for revoked certificates [30]. MMA developers should ensure that back-end APIs within mobile platforms are strengthened against attacks using state of the art encryption. As discussed above a MMA could expose healthcare systems that had not previously been accessible from outside their own networks. In MMA data security consideration developers should always use modern encryption algorithms that are accepted as strong by the security community.

Hackers are aware that just because a patch was released does not means it was applied, which, in turn make the app vulnerable for attacks [31]. Some recommend the installation of "Prevention and Detection" software for defending and protecting against malware as essential [25]. Consequently, software that tracks detection and anticipates attacks would require consideration in MMA development.

It is essential that developers research the mobile platforms they are developing for. Each mobile OS offers different security-related features, uses different APIs and handles data permissions its own way. Developers should adapt the code accordingly for each platform the MMA will

be run on. There are no standards that straddle development or security testing across the different platforms. Developers design security for each individual OS.

III. Privacy and Security Laws for Health Data

In the rush to market the aspects of privacy and security are not properly considered [32]. Increasingly, MMA developers must deal with a range of international regulations if they want to perform business in more than one country. The absence of privacy laws in some countries, in addition to inconsistency or even conflicting laws, means PHI is often misused and treated superficially. Some MMA providers find they are in breach of regulation only when they are warned or fined, blindsided by regulatory issues, due to the complexity [33]. Privacy and security policy issues relating to data with MMAs are now of primary importance since the surge in the value of PHI on the black-market partly due to the lack of security controls within healthcare and the increase in the security of credit card data [34]. A global landscape analysis of current privacy legislation and regulation was undertaken by Thomas Reuters Foundation and mHealth Alliance on the privacy and security policies to protect health data [33]. The report states, that most jurisdictions agree, data security is essential and suggests the world of privacy law is divided into three major groups: Omnibus data protection regulation in the style of the European laws that regulate all personal information equally; U.S.-style sectorial privacy laws that address specific privacy issues arising in certain industries and business sectors, so that only certain types of personal information are regulated; The constitutional approach, whereby certain types of personal information are considered private and compelled from a basic human rights perspective but no specific privacy regulation is in place otherwise [33].

A. European Union

If you have MMAs within the EU, the EU Data Protection Directive (Directive 95/46/EC) [35] is the key piece of regulation that will affect how you manage and store data. This is the one law in the EU regarding security and privacy in health data. This Directive is implemented in laws of Member States and requires establishment of supervisory authorities to monitor its application. However, at the beginning of 2012, the EU approved the draft of the European Data Protection Regulation [36]. This means the law will apply generally over all states in the EU, so it will not require individual Member States implementation. With this progression in regulation all Member States will be at the same stage of security and data protection [32]. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 [37], known as the ePrivacy Directive, is concerned with the processing of personal data and the protection of privacy in the digital age. It is now law in all EU countries and covers all non-essential cookies, and tracking devices. This Directive principally concerns the processing of personal data relating to the delivery of communications services. It provides rules on how providers of electronic communication services, should manage their subscribers' data. It also guarantees rights for subscribers when they use these services. The key parts that MMA developers are concerned with in the directive are: processing security; confidentiality of communication; processing traffic and location data; cookies and controls.

B. United States

According to the Thomas Reuters Foundation and mHealth Alliance report, the US is one of the legislative leaders in this area [33]. The main law that applies to health data issues is HIPAA as stated previously. HIPAA was updated in the HIPAA Omnibus Rule required by The Health Information Technology for Economic and Clinical Health Act of 2010, (HITECH Act). The HITECH Act established new information security breach notification requirements that apply to businesses that handle personal health information and other health data [38]. The FDA released guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" and this provides a list of recognized consensus standards dealing with Information Technology and medical device security [39]. The fact that MMAs may transmit information wirelessly places them in the domain of Federal Communications Commission (FCC) regulation to ensure consumer and public safety [40]. Recognizing the need for regulatory clarity, the FCC, FDA, Office of the National Coordinator (ONC) and the Department of Health and Human Services (HHS) came together in a grouping called the Food and Drug Administration Safety and Innovation Act (FDASIA) Working Group. The group released a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology including MMAs [41].

IV. Proprosed Current Research

A. Research Background

As the MMA domain grows and becomes a standard established mechanism for health delivery, data security and privacy of health data will be essential. MMAs are being developed persistently without proper security application, principally due to the lack of understanding of current standards, regulation requirements and best practice pertaining to data security in healthcare. There are currently no process models or testing suites for developers to assure data security in transmission for MMAs.

The proposed research is developed using the only Medical Device (MD) security standard, IEC/TR 80001-2-2:2012. This standard presents 19 high-level security-related capabilities in understanding the type of security controls to be considered and the risks that lead to the controls [42]. IEC/DTR 80001-2-8 (currently at a committee draft stage) is a catalogue of security controls developed relating to the security capabilities defined in IEC/TR 80001-2-2. The report presents mapping of security controls for developing security cases to establish confidence in each of the security capabilities [43]. Accordingly, the security controls support the maintenance of confidentiality and protection from malicious intrusion. The report provides guidance to healthcare organizations and MD manufacturers for the

selection of security controls to protect the CIA and accountability of data and systems during development, operation and disposal [43].

This research leverages on the established security controls in IEC/WD TR 80001-2-8 relating to the two transmission security capabilities from IEC/TR 80001-2-2. We will also apply additional security controls pertinent to MMAs, accomplished with comparative expert validation, by means of analysis of applicable standards and best practices. Further, we will research to adopt testing methods and applicable tests to form a testing suite, in collaboration with a data security expert to assure that the required security controls for data CIA in data transmission are in place.

B. Approach

The research will be completed in three parts. The research method will consist of Literature Review (LR) and Action Design Research (ADR) for each part.

1) Approach part one: The two transmission security capabilities selected from IEC/WD 80001-2-2 will provide the starting point. The catalogue of security controls in IEC/WD 80001-2-8 for the two capabilities will provide the basis for the security controls. The LR for this part will establish the additional standards and best practices pertaining to mobile data transmission and security of data. To develop the process to establish the security controls applicable to MMAs. Some of the standards and best practices currently being research include (but not inclusive) are: ISO/IEC 11073; NIST SP 800-53, OWASP mobile security; NIST FIPS 140-2; ISO 27799. The LR will additionally review other domains that have experience in data security in transmisssion, e.g., financial, to establish practices. The ADR fragment will develop and validate the process with comparitive expert review.

2) Approach part two: A LR will establish the current cyber attacks on mobile apps, MDs and MMAs and establish a database. The LR will additionally research testing methods associated with the attacks and applicable tests. This part will be completed in collaboration with identified data security experts and a testing organisationation. To assure that the required security controls for data CIA in data transmission are in place. The Testing Suite will be complied through ADR via the data experts, testing organisation and MMA developers.

3) Approach part three; The completion of the research will be through ADR with two identified MMA development companies. The development of the Process Model and the Testing suite will be validated through ADR with industrial partners. Completion of the research aim is the demonstration of confidence of data security during transmission MMAs. Therefore demonstrating confidence/trust in the data transmission and storage.

V. Conclusion and Future Work

This paper examined existing data security issues and practices in relation to MMAs. A summary of regulations relating to data privacy and security MMA providers are mandated by law to adhere to, were outlined. Compliance and improved understanding of data security regulations and best practices will assist developers to meet the security requirements for data in transmission. The security gaps in MMAs are exploited due to lack of knowledge, understanding or amalgamated regulation for data security with MMAs.

The mobile app industry claim innovation is stifled, due to the lack of clarity in regulations and security concerns. Developers will need to find the optimal balance between data security and privacy as MMAs expand and PHI enters into new aspects. The lack of consistent data security to assure privacy, to allow interoperability, and to maximize the full capabilities [44] of presents a significant barrier to the industry. The primary focus of our future research in this domain will be in the development and implementation of both the process model and testing suite. Validation of the research will be completed in collaboration with two MMA development companies. The MMAs being developed will have different transmission requirements and capabilities to assure diversity.

Acknowledgment

This research is supported by the Science Foundation Ireland through Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855 and grant 13/RC/20194.

References

[1] B. M. Silva, J. P. C. Rodrigues, F. Canelo, I. C. Lopes, and L. Zhou, “A data encryption solution for mobile health apps in cooperation environments.,” J. Med. Internet Res., vol. 15, no. 4, p. e66, Jan. 2013, doi:10.2196/jmir.2498.

[2] D. He, M. Naveed, C. A. Gunter, and K. Nahrstedt, “Security Concerns in Android mHealth Apps,” In AMIA Annual Symposium Proceedings. Nov. 2014, pp. 645–654.

[3] Y. Yang and R. . Sliverman, “‘Mobile health applications: the patchwork of legal and liability issues suggests strategies to improve oversight.,’” Health Aff., vol. 33, no. 2, pp. 222–7, 2014, doi: 10.1377/hlthaff.2013.0958.

[4] Price Waterhouse Cooper - Health Research Institute, “Top Health Industry Issues of 2015 - A new health economy takes shape,” Nov. 2014. pp. 1-18.

[5] “Data breach results in $4.8 million HIPAA settlements,” U.S. Department of Health and Human Services, 2014. [Online]. Available from: http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html 2016.01.10

[6] N. H. Ab Rahman, “Privacy disclosure risk: smartphone user guide,” Int. J. Mob. Netw. Des. Innov., vol. 5, no. 1, pp. 2–8, 2013, doi: 10.1504/IJMNDI.2013.057147.

[7] G. S. McNeal, “Health Insurer Anthem Struck By Massive Data Breach - Forbes,” Forbes, 2015. [Online]. Available from: http://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/ 2016.01.10

[8] U.S. FDA “Safety Communications - Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication.” FDA Website, 2013 [Online]. Available from:http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm 2016.01.10

[9] FBI, “Internet of Things Poses Opportunities for Cyber Crime,” FBI Website, 2015. [Online]. Available from: https://www.ic3.gov/media/2015/150910.aspx 2016.01.10

[10] J. Williams, “Don’t Mug Me For My Password! - InformationWeek,” Information Week, 2014. [Online]. Available:http://www.informationweek.com/healthcare/security-and-privacy/dont-mug-me-for-my-password!/a/d-id/1318316 2016.01.10

[11] Araxan, “State of Mobile App Security,” Volume 3, Nov 2014.

[12] J. Kabachinski, “Mobile medical apps changing healthcare technology.,” Biomed. Instrum. Technol., vol. 45, no. 6, pp. 482–6, Nov/Dec. 2011, doi: 10.2345/0899-8205-45.6.482

[13] European Commission, “Green Paper on mobile Health (‘mHealth’),” Brussels, 2014.

[14] U.S. FDA, “Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff,” 2013.

[15] M. La Polla, F. Martinelli, and D. Sgandurra, “A Survey on Security for Mobile Devices,” Commun. Surv. Tutorials, IEEE vol. 15, no. 1, 2013, pp. 446–471.

[16] M. Al Ameen, J. Liu, and K. Kwak, “Security and privacy issues in wireless sensor networks for healthcare applications.,” J. Med. Syst., vol. 36, no. 1, pp. 93–101, Feb. 2012, doi: 10.1007/s10916-010-9449-4.

[17] J. Y. Khan and M. R. Yuce, “Wireless Body Area Network (WBAN) for Medical Applications,” in New Development in Biomedical Engeneering, D. Campolo, Ed. InTech, pp. 591–623, 2010.

[18] S. Saleem, S. Ullah, and K. S. Kwak, “A study of IEEE 802.15.4 security framework for wireless body area networks.,” Sensors (Basel)., vol. 11, no. 2, pp. 1383–95, Jan. 2011, doi: 10.3390/s110201383.

[19] J. L. Hall and D. McGraw, “For Telehealth to Succeed, Privacy and Security Risks Must be Identified and Addressed,” Health Aff., vol. 33, no. 2, pp. 216–221, 2014, doi: 10.1377/hithaff.2013.0997

[20] Ponemon Institute LLC, “The State of Mobile Application Insecurity,” IBM, 2015.

[21] V. Mainanwal, M. Gupta, and S. Kumar Upadhayay, “A Survey on Wireless Body Area Network : Security Technology and its Design Methodology issue,” in 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS 2015), IEEE, March 2015, no. I, pp. 1–5, ISBN: 9781479968183

[22] S. S. Kim, Y. H. Lee, J. M. Kim, D. S. Seo, G. H. Kim, and Y. S. Shin, “Privacy Protection for Personal Health Device Communication and Healthcare Building Applications,” J. Appl. Math., vol. 2014, pp. 1–5, June 2014, doi: 10.1155/2014/462453

[23] M. Souppaya and K. Scarfone, NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise. Gaithersburg, USA: National Institute of Standards and Technology, 2013, pp. 1–29.

[24] D. Nyambo, Z. O. Yonah, and C. Tarimo, “Review of Security Frameworks in the Converged Web and Mobile Applications,” Int. J. Comput. Inf. Technol., vol. 3, no. 4, pp. 724–730, Jul. 2014.

[25] A. S. Alqahtani, “Security of Mobile Phones and their Usage in Business,” Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 11, pp. 17–32, 2013.

[26] C. Wiltz, “Mobile App Developers to Congress: HIPPA is Stifling Innovation | MDDI Medical Device and Diagnostic Industry News Products and Suppliers,” Mobile Health, 2014. [Online]. Available from: http://www.mddionline.com/article/mobile-app-developers-congress-hippa-stifling-innovation-140918 2016.01.10

[27] FierceHealthIT, “Mobile & HIPAA Securing personal health data in an increasingly portable workplace.” FierceHealthIT, 2014. [Online]. Available from: http://servicecenter.fiercemarkets.com/files/leadgen/mobile_and_hipaa_final.pdf 2016.01.10

[28] P. Ruggiero and J. Foote, “Cyber Threats to Mobile Phones,” United States Computer Emergency Readiness Team, 2011.

[29] H. Xue, T. Wei, and Y. Zhang, “Masque Attcak: All Your iOS Apps Belong to US,” FireEye, 2014. [Online]. Available from: https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html 2016.01.10

[30] M. B. Barcena, C. Wueest, and H. Lau, “How safe is your quantified self” Symantech: Mountain View, CA, USA 2014.

[31] Y. S. Baker, R. Agrawal, and S. Bhattacharya, “Analyzing Security Threats as Reported by the United States Computer Emergency Readiness Team,” International Conference on Intelligence and Security Informatics (ISI 2013) IEEE, June 2013, pp. 10–12, ISBN:978-1-4673-6214-6

[32] B. Martinez-Perez, I. Torre-Diez de la, and M. Lopez-Coronado, “Privacy and Security in Mobile Health Apps: A Review and Recommendations,” J. Med. Syst., vol. 39, no. 1, p. 1-8, Jan. 2015, doi: 10.1007/s10916-014-0181-3

[33] Thomas Reuters Foundation and mHealth Alliance, “Patient Privacy in a Mobile World a Framework to Address Privacy LawIssues in Mobile Health,” Thomas Reuters Foundation, London, 2013.

[34] J. Williams, “Don’t Mug Me For My Password! - InformationWeek,” Information Week Healthcare, 2014. [Online]. Available from: http://www.informationweek.com/healthcare/security-and-privacy/dont-mug-me-for-my-password!/a/d-id/1318316 2016.01.10

[35] Directive, E.U. "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Official Journal of EC 23.6, 1995.

[36] EU Commission. "Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (Vol. 11) 2012.

[37] Directive, E.U. "2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Off." (Directive on privacy and electronic communications). JL 201, 31.7. 2002.

[38] L. J. Sotto, B. C. Treacy, and M. L. Mclellan, “Privacy and Data Security Risks in Cloud Computing,” Electron. Commer. Law Rep., vol. 186, pp. 1–6, Feb. 2010.

[39] U.S. Food and Drug Administration, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff,” 2014.

[40] A. A. Atienza and K. Patrick, “Mobile Health: The Killer App for Cyberinfrastructure and Consumer Health,” Am. J. Prev. Med., vol. 40, pp. 151–153, May 2011.

[41] Food and Drug Administration and Safety and Innovation Act (FDASIA), “FDASIA Health IT Report Proposed Strategy and Recommendations for a Risk-Based Framework,” 2014.

[42] IEC/TR 80002-2-2:2012, Application of risk management for IT-networks incorporating medical devices Part 2-2 : Guidance for the disclosure and communication of medical device security needs, risks and controls. 2012.

[43] A. Finnegan and F. McCaffery, “A security Argument for Medical Device Assurance Cases,” Softw. Reliab. Eng. Work. (ISSREW), IEEE Int. Symp., Nov. 2014, pp. 220–225.

[44] European Commission, “Medical Devices: Guidance Document MEDDEV 2.1/1.” 2012.